APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/693,713	10/19/2000	Kunihiko Miyazaki	16869P-011500	7398

20350	7590	05/12/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER
HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 October 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2, 3, 6, and 7*.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Priority

1.   Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which

papers have been placed of record in the file.

Drawings

2.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5)

because they do not include the following reference sign(s) mentioned in the

description:

- Reference numbers 131 and 132, on page 7, lines 26 and 29, respectively.

- Reference numbers 331 and 332, on page 8, lines 5 and 7, respectively.

- Throughout the specification there are 3-digit reference numbers that refer to

    parts that are never shown in the drawings. Two examples were shown above,

    however, more exist throughout the specification. The Examiner finds that any 3-

    digit number, excluding numbers between 200-299, exist in the specification, but

    not in the drawings.

- Reference number 9, on page 16, line 25.

A proposed drawing correction or corrected drawings are required in reply to the Office

action to avoid abandonment of the application. The objection to the drawings will not

be held in abeyance.

Specification

3.   The disclosure is objected to because of the following informalities:

- On page 1, lines 6 and 12, the heading is repeated twice. One of these headings needs changed.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent, or

5.   <u>Claims 1-6, 13-20, 27-29, 31, and 32</u> are rejected under 35 U.S.C. 102(a) as being anticipated by <u>Schneier et al.</u> (U.S. Patent No. 5,956,404).

    Regarding <u>claims 1, 13, and 27</u>, <u>Schneier et al.</u> teaches a digital signing method/apparatus/computer program, comprising:

- A processor (col. 5, lines 22-28); and

- A storage medium (col. 5, lines 28-35);

- Wherein said processor applies a secret key to a message to generate a digital signature for the message (col. 5, lines 7-9); and

- Wherein said processor prepares a digital-signature-attached message including the generated digital signature and the message (col. 5, lines 35-41); and

- Wherein said processor registers log data of said digital-signature-attached message with a log list in said storage medium (col. 11, lines 30-42).

Regarding claim 28, Schneier et al. teaches wherein the computer readable storage medium is a computer readable medium for storing the codes (col. 5, line 26).

Regarding claim 29, Schneier et al. teaches wherein the computer readable storage medium is a computer readable medium for transmitting the codes (col. 5, line 26).

Regarding claims 2 and 14, Schneier et al. teaches wherein said message is a hash value of another message (col. 6, line 65 through col. 7, line 15).

Regarding claims 3 and 15, Schneier et al. teaches:

- Wherein said processor applies said secret key to a message and data from a previously signed message retrieved from a recent log data registered in said log list to generate a digital signature for the message (col. 11, lines 30-64); and

- Wherein said processor prepares a digital-signature-attached message that includes the generated digital signature, the message and the data from a previously signed message (col. 11, lines 54-60); and

- Wherein said processor registers log data of a digital-signature-attached message including the generated digital signature, the message, and the data from a previously signed message, with said log list (col. 11, lines 50-53).

Regarding <u>claims 4 and 16</u>, <u>Schneier et al.</u> teaches wherein:

- Said log data further comprises a distribution destination (col. 6, lines 27-29), and

- Wherein said processor registers log data of a digital-signature-attached

  message with a log list, said log data including a distribution destination attached

  thereto (col. 11, lines 30-42).

Regarding <u>claims 5 and 17</u>, <u>Schneier et al.</u> teaches wherein registration of the

log data with said log list is permitted only when the data from a previously signed

message included in said digital-signature-attached message is included in the latest

log data registered with said log list (col. 11, lines 45-48).

Regarding <u>claims 6 and 18</u>, <u>Schneier et al.</u> teaches

- Wherein said processor obtains a timestamp from a trusted authority, said

  timestamp generated by applying a second secret key to the digital signature,

  and a time (col. 12, lines 41-48); and

- Said processor prepares said digital-signature-attached message including the

  generated digital signature, the timestamp, and the message (col. 12, lines 45-47

  and fig. 3, ref. num 285).

Regarding <u>claim 19</u>, <u>Schneier et al.</u> teaches further comprising an interface

configured to be connectable to a computer (col. 5, lines 24-28).

Regarding <u>claim 20</u>, <u>Schneier et al.</u> teaches:

- Wherein if a number of the log data registered with the log list exceeds a particular value, said processor outputs at least one of a plurality of log data registered with the log list to said computer, whereupon said computer registers said at least one of a plurality of log data with a second log list prepared in said computer (col. 11, lines 5-13), and thereupon,

- Said processor deletes said at least one of a plurality of log data from said log list in said storage medium (col. 11, lines 13-15).

Regarding <u>claim 31</u>, <u>Schneier et al.</u> teaches a digital timestamp issuing apparatus, comprising:

- A processor and an interface (col. 5, lines 22-28),

- Wherein said processor generates a timestamp by applying a secret key to data received by said interface (col. 10, lines 30-34),
    - Said data comprising a digital signature sent from a digital signer, and a reception time of the digital signature (col. 10, lines 34-37); and

- Wherein said processor transmits said timestamp to said digital signer using said interface (col. 10, lines 34-37).

Regarding <u>claim 32</u>, <u>Schneier et al.</u> teaches a digital signing system, said system comprising:

- A digital signing apparatus (col. 5, lines 7-34);

- A timestamp issuing apparatus (col. 10, lines 30-37);

- Said digital signing apparatus comprising a processor and a communication interface (col. 5, lines 22-28),

  o Wherein said processor applies a first secret key to a message or its hash value to generate a digital signature (col. 5, lines 7-9); and

- Said processor transmits said digital signature to said timestamp issuing apparatus by said communication interface and acquires a timestamp in response (col. 10, lines 44-50); and

- Wherein said processor attaches the acquired timestamp to said message to create a digital-signature-attached message (col. 12, lines 45-47 and fig. 3, ref. num 285); and

- Said timestamp issuing apparatus comprising a processor and a communication interface (col. 5, lines 22-28),

- Wherein said processor generates a timestamp by applying a second secret key to data which includes the digital signature sent by said digital signing apparatus, and a reception time of the digital signature (col. 10, lines 30-34); and

- Wherein said processor transmits said timestamp to said digital signing apparatus (col. 10, lines 34-37).

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7.   Claims 7-12, 21-26, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (U.S. Patent No. 5,978,475), hereinafter referred to as '475, in view of Schneier et al. (U.S. Patent No. 5,956,404), hereinafter referred to as '404.

Regarding claims 7, 21, and 30, '475 teaches a digital signature verifying method/apparatus/computer program, comprising:

- A processor interconnected with an input device (fig. 1B, ref. num 110 to 180);

- Accepting a message (col. 13, lines 15-16);

- Acquiring a log list of a digital signer (col. 13, lines 17-22); and

- Checking whether log data of said digital-signature-attached message is registered in said log list (col. 13, lines 23-33),

- And if the log data is registered in the log list, authenticating that the digital-signature-attached message was distributed by the digital signer (col. 13, line 65 through col. 14, line 1).

'475 does not specifically teach the accepting is of a digital-signature-attached message, wherein said digital-signature-attached message may have been distributed by said digital signer is to be verified.

'404 teaches accepting a digital-signature-attached message (col. 5, lines 35-41),

wherein said digital-signature-attached message may have been distributed by said

digital signer is to be verified (col. 11, lines 45-48).

It would have been obvious to one of ordinary skill in the art, at the time the

invention was made, to combine accepting a digital-signature-attached message,

wherein said digital-signature-attached message may have been distributed by said

digital signer is to be verified, as taught by '404, with the method/apparatus/computer

program of '475. It would have been obvious to combine accepting a digital-signature-

attached message, wherein said digital-signature-attached message may have been

distributed by said digital signer is to be verified, as taught by '404, with the method/

apparatus/computer program of '475 because a digital-signature-attached message

provides a strong audit trail; a strong audit trail provides an indisputable list of actions to

verify all events that took place.

Regarding claims 8 and 22, the combination of '475 in view of '404 teaches said

method further comprising checking whether the digital signature included in the

digital-signature-attached message has been generated for the message included in the

digital-signature-attached message, using the digital signature and the message

included in said digital-signature-attached message and a public key paired with a

secret key of said digital signer (see col. 15, lines 1-8 of '475).

Regarding <u>claims 9 and 23</u>, the combination of <u>'475</u> in view of <u>'404</u> teaches:

- Wherein said digital-signature-attached message further comprises data from a previously signed message (see col. 11, lines 30-64 of '404),

- Said method further comprising checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature, the data from a previously signed message, and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer (see col. 15, lines 12-15 of '475).

Regarding <u>claims 10 and 24</u>, the combination of <u>'475</u> in view of <u>'404</u> teaches said method further comprising checking whether data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before log data of said digital-signature-attached message in said log list, and if the data from a previously signed message is included in the immediately previous registered log data, authenticating that said log list has not been altered (see col. 11, lines 45-48 of '404).

Regarding <u>claims 11 and 25</u>, the combination of <u>'475</u> in view of <u>'404</u> teaches:

- Wherein said log data further comprises a distribution destination (see col. 6, lines 27-29 of '404),

- Said method further comprising acquiring a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list (see col. 11, lines 30-42 of '404), and

- Checking whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, authenticating that said log list has not been altered (see col. 11, lines 44-50 of '404).

Regarding claims 12 and 26, the combination of '475 in view of '404 teaches:

- Wherein said digital-signature-attached message further comprises a timestamp created using a second secret key (see col. 12, lines 41-48 of '404),

- Said method further comprising acquiring a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message (see col. 12, line 65 through col. 13, line 1 of '404); and

- Checking whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message (see col. 12, lines 49-59 of '404),

- And if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, authenticating the validity of the acquired digital signature (see col. 12, line 59-65 of '404).

Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier

et al. (U.S. Patent No. 5,956,404) in view of Schneier et al. (U.S. Patent No. 5,978,475).

Regarding claim 33, Schneier et al. '404 teaches said system further comprising

a digital signature verifying apparatus comprising said processor checks whether date

and time indicated by the time data exceeds expiration date and time assigned at said

digital signing apparatus (see col. 12, lines 49-59 of '404), and when the date and time

indicated by the time data does not exceed the expiration date and time, said processor

authenticates the validity of the said digital signature (see col. 12, line 59-65 of '404).

Schneier et al. '404 does not teach a processor interconnected with an input

device, wherein said input device accepts a digital-signature-attached message to be

verified, wherein said processor acquires a digital signature and time data by applying a

public key paired with the secret key of the timestamp apparatus to the timestamp

included in said digital-signature-attached message, said processor authenticates

whether said digital signature included in said digital-signature-attached message has

been generated for the message included in said digital-signature-attached message,

using said digital signature, the message included in said digital-signature-attached

message, and a public key paired with the secret key of the digital signing apparatus.

Schneier et al. '475 teaches:

- A processor interconnected with an input device (fig. 1B, ref. num 110 to 180),

    o Wherein said input device accepts a digital-signature-attached message to be verified (col. 13, lines 15-33);

- Wherein said processor acquires a digital signature and time data by applying a public key paired with the secret key of the timestamp apparatus to the timestamp included in said digital-signature-attached message (col. 15, lines 1-8),

- Said processor authenticates whether said digital signature included in said digital-signature-attached message has been generated for the message included in said digital-signature-attached message, using said digital signature, the message included in said digital-signature-attached message, and a public key paired with the secret key of the digital signing apparatus (col. 15, lines 1-8).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine accepting a digital-signature-attached message, wherein the processor authenticates if the message is for the current digital-signature-attached message by using the digital signature and a public key paired with the secret key of the signing apparatus, as taught by '475, with the system of '404. It would have been obvious to combine accepting a digital-signature-attached message, wherein the processor authenticates if the message is for the current digital-signature-attached message by using the digital signature and a public key paired with the secret key of the signing apparatus, as taught by '475, with the system of '404 because the system provides a verifying machine a secure audit log for a trusted machine and an un-trusted

machine. By using a public key and a corresponding secret key, the audit log can only be viewed by its intended recipient.

Conclusion

8.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. U.S. Patent No. 6,397,332 to Kawano et al. verifies a current digital signature based on previous entries in a digital signature log.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100